Multihop Sensor Network Design for Wide-Band Communications

HAMID GHARAVI, FELLOW, IEEE, AND KOICHIRO BAN, MEMBER, IEEE

Invited Paper

This paper presents a master/slave cellular-based mobile ad hoc network architecture for multihop multimedia communications. The proposed network is based on a new paradigm for solving the problem of cluster-based ad hoc routing when utilizing existing wireless local area network (WLAN) technologies. The network architecture is a mixture of two different types of networks: infrastructure (master-and-slave) and ad hoc. In this architecture, the participating slave nodes (SNs) in each cluster communicate with each other via their respective master nodes (MNs) in an infrastructure network. In contrast to traditional cellular networks where the base stations are fixed (e.g., interconnected via a wired backbone), in this network the MNs (e.g., base stations) are mobile; thus, interconnection is accomplished dynamically and in an ad hoc manner. For network implementation, the IEEE 802.11 WLAN has been deployed. Since there is no stationary node in this network, all the nodes in a cluster may have to move together as a group. However, in order to allow a mobile node to move to another cluster, which requires changing its point of attachment, a handoff process utilizing Mobile IP version 6 (IPv6) has been considered. For ad hoc routing between the master nodes (i.e., MNs), the Ad hoc On-demand Distance Vector (AODV) Routing protocol has been deployed. In assessing the network performance, field test trials have been carried out to measure the proposed network performance. These measurements include packet loss, delays under various test conditions such as a change of ad hoc route, handoffs, etc.

Keywords*—Ad hoc networks, cluster networks, IEEE 802.11, mobile IP, wireless local area network (WLAN).*

I. Introduction

Motivated by the growing need for multimedia applications such as video image and data, multihop ad hoc networking is emerging as a viable technology for many civilian, military, as well as commercial applications. For instance, wireless ad hoc networks can be deployed in situations where there is no communications infrastructure or the existing communications infrastructure might have been destroyed. Such endeavors include emergency response to natural disasters, bomb threats, search and rescue, cleanup operations, etc. Under these conditions, a team of high-performance robots capable of transmitting video and other sensor data can be rapidly deployed.

To provide a large coverage area for such applications, multihop communication has been vastly favored over long-range single-hop links. The use of multihop is to combat the rapid decay of the electromagnetic received signal strength as communication distance increases. In addition, multihop communication between distributed mobile nodes offers pathways around electromagnetic transmission obstacles that would otherwise prevent the formation of a long-range network. Another important factor is that the high-performance sensor network for video communications would require broad-band/wide-band links so that it can distribute video for a large number of nodes within a coverage area. Unfortunately, the deployment of a large number of nodes operating in an ad hoc mode would severely constrain the performance of a routing protocol and consequently affect the reliability of the linkage. In order to reduce the number of ad hoc nodes in this paper, a new cluster-based network architecture has been proposed. Such a network is based on the assumption that different sets of nodes move as a group and the network should be capable of providing handoff for isolated nodes moving from one cluster to another. To implement the proposed network, existing wireless local area network (WLAN) technologies have been used to provide wide-band access for multimedia communications.

In this paper, we present the design aspects of the proposed network architecture. Section II introduces the proposed cluster-based mobile ad hoc network for IP version 4 (IPv4), as well as a brief description of the ad hoc routing protocol used for our experiments. The handoff aspects, where a node changes its point of attachment using IP version 6

Manuscript received October 2, 2002; revised March 12, 2003. This work was supported by the Defense Advanced Research Projects Agency (DARPA) SensIT under Grant L.738.

The authors are with the National Institute of Standards and Technology, Gaithersburg, MD 20899-8920 USA (e-mail: gharavi@nist.gov).

Digital Object Identifier 10.1109/JPROC.2003.814919

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **AUG 2003**	2. REPORT TYPE	3. DATES COVERED **00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE **Multihop Sensor Network Design for Wide-Band Communications**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Institute of Standards and Technology,Gaithersburg,MD,20899**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

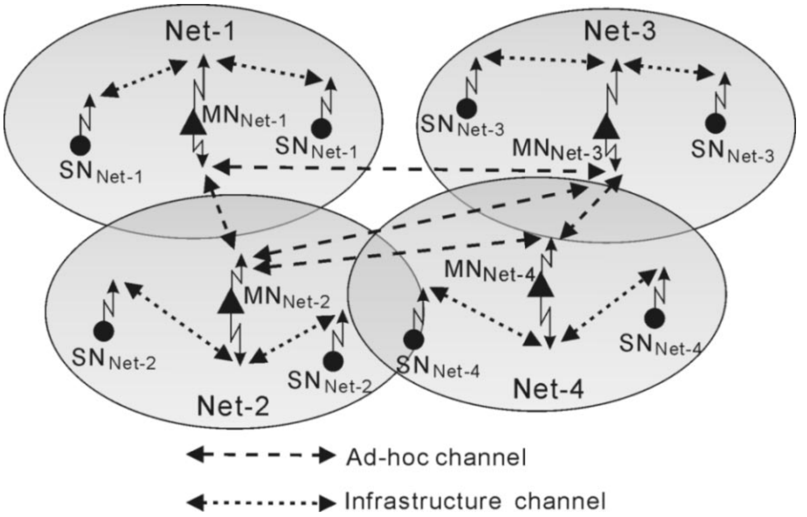


Fig. 1. Master/slave cluster-based mobile ad hoc network.

(IPv6), are presented in Section III. Section IV presents a brief overview of the IEEE 802.11 b WLAN technology that was used in implementing the proposed network. Finally, the paper presents the experimental testbed to measure the effect of a route change and handoffs. The network performance is presented in terms of multihop delays, handoff delays, and packet-loss rates under full mobility conditions.

II. Proposed Cluster-Based Network

The concept of cluster-based networking has been extensively studied in the past several years [1]–[5]. This concept is based on dynamically selecting a cluster head among the active nodes. The main drawback of this approach is the routing complexity (as the number of nodes increases), network management, and large overheads that may become a bottleneck in a cluster [5]. Although there has been considerable effort in recent years to improve the routing performance and reduce the overhead, in this paper we present a simple yet easily implementable cluster-based networking scheme. The network architecture utilizes existing WLAN technologies and, thus, can provide wide-band access for multimedia communications [20], [21]. The proposed network implementation is based on a master/slave network architecture where the ad hoc routing would involve only the master nodes.

Fig. 1 illustrates a basic network configuration for a master/slave cluster-based network. The proposed architecture consists of two types of networks: infrastructure (managed) and ad hoc. In addition, there are two types of nodes in this network: master node (MN) and slave node (SN). The MN, which operates as a moving base station in a cluster, communicates with its slave nodes in an infrastructure mode. Communications among the MNs are performed in an ad hoc manner.

For implementation, IEEE 802.11 b [6] WLAN access point (AP) can be used to represent a mobile MN. However, the main difficulty is that the AP cannot operate in an ad hoc mode for communicating with other MNs. To overcome this problem, we have designed a simple architecture that can allow an AP to work in an ad hoc mode (e.g., achieving a protocol conversion from infrastructure to ad hoc mode). In this architecture, packets that are received by an AP are routed via a LAN interface to a wireless LAN card (using PDA or laptop) so that it can operate in an ad hoc mode. As will be shown later (see Fig. 2), an MN consists of an AP, a LAN interface, and a wireless LAN card (e.g., using laptop or PDA devices), whereas an SN uses only a wireless LAN card (e.g., using PDA). In this network, only SNs operate in an infrastructure mode and, thus, are allowed to associate with only one AP at a time [7]. In addition, since in this architecture there is no stationary node, every master node (MN) acts as a mobile base station. This would require a special arrangement for ad hoc routing, which will be discussed next.

A. Network Implementation

For the infrastructure network using IPv4 configuration, Fig. 2 shows an example of class C private IPv4 addressing for a network of four clusters [7]. Each cluster has been assigned to a unique network address (network suffix). For example, for a network of n clusters, 192.168.1.0 is allocated to cluster 1 (Net-1), 192.168.2.0 to cluster 2 (Net-2), and $192.168.n.0$ to cluster n (Net-n) and so on. Under this arrangement, SNs in Net-1 can use IP addresses ranging from 192.168.1.2 to 192.168.1.244. Similarly, for Net-n, the range would be between $192.168.n.2$ to $192.168.n.244$. Note that $192.168.x.1$ $(x = 1, 2, \ldots, n)$ has been allocated to the LAN interface, which is connected to the AP, of the MN in Net-x $(\mathrm{MN}_{\mathrm{Net}\text{-}x})$. In addition, we assigned $192.168.0.x$ $(x = 1, 2, \ldots, n)$ to the WLAN interface of the $\mathrm{MN}_{\mathrm{Net}\text{-}x}$ for operation in an ad hoc mode between the MNs. This network will be referred as Net-0 in this paper.

As an example, let us consider the scenario depicted in Fig. 3, where the correspondent SN (SN-S) in cluster 1 (Net-1) with IP address 192.168.1.2 want to send packets to the receiving SN (SN-D) in cluster 3 (Net-3) with IP address 192.168.3.2. Since the SN-S can communicate only through its associated MN in Net-1 $(\mathrm{MN}_{\mathrm{Net}\text{-}1})$, the gateway to other network addresses is always the infrastructure interface

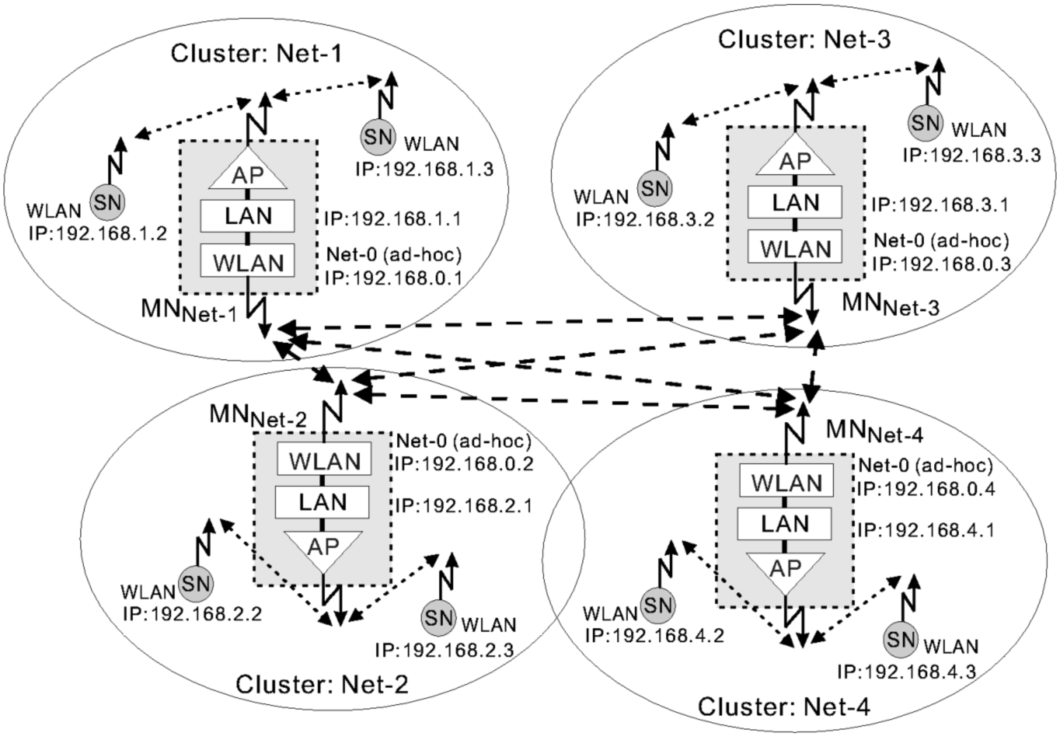


Fig. 2. IPv4 addressing for infrastructure/ad hoc networking.

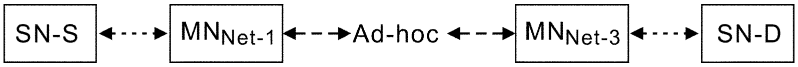


Fig. 3. End-to-end system using infrastructure/ad hoc routing.

in the MN_{Net-1} (i.e., 192.168.1.1). In this configuration, suppose an ad hoc routing protocol is utilized for the WLAN interfaces in MNs. As the SN-D is not in the same cluster as SN-S, the MN_{Net-1} must find the route to the MN_{Net-3} for sending the packets to SN-D.

Since the cluster of Net-3 is known by the IP address of MN_{Net-3}, the responsibility of an ad hoc routing protocol is to find a route from the MN_{Net-1}: 192.168.0.1 to the MN_{Net-3}: 192.168.0.3. Once the route is established, the packets from the SN-S are transmitted to the MN_{Net-3} via the MN_{Net-1} and then forwarded to their final destination SN-D.

However, the main difficulty with this arrangement is that not all nodes in this network are ad hoc nodes (see Fig. 3). Under this condition, IP packets received by one MN (e.g., MN_{Net-1}) cannot be directly routed to another MN (e.g., MN_{Net-3}) via an ad hoc routing protocol. In other words, as far as routing protocols are concerned, MNs should be regarded as the only mobile nodes in the network. Thus, in order to solve this problem, we developed a tunneling technique where packets that are locally received by an MN are encapsulated using the Net-0 IP address header. Under this arrangement, packets can now be forwarded to their destination MN in an ad hoc mode. For instance, if MN_{Net-1} receives packets from one of its slave nodes (e.g., SN-S) destined to another slave node (SN-D), which is attached to MN_{Net-3}, the packets should first be encapsulated at MN_{Net-1} using Net-0 addressing. Fig. 4 shows such tunnelling arrangements for a network of three clusters. As shown in this example, the encapsulated packets use MN_{Net-3}: 192.168.0.3 as the destination address and MN_{Net-1}: 192.168.0.1 as the source address. Subsequently,

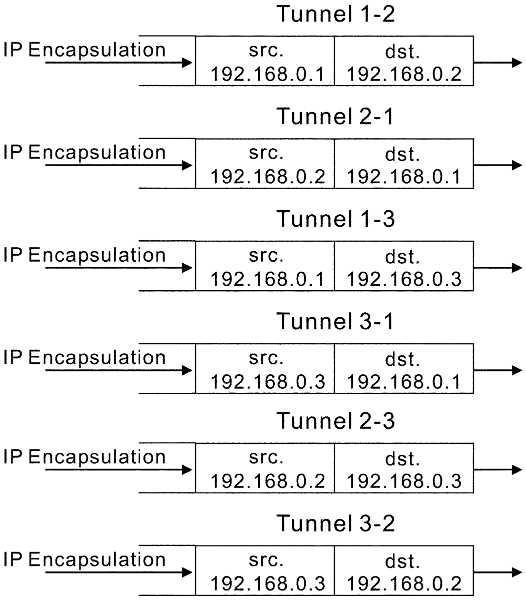


Fig. 4. Example of creating tunneling arrangements for a network of three clusters.

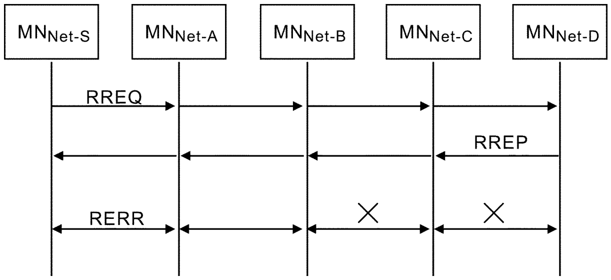


Fig. 5. AODV multihop routing example.

packets received at MN$_{\text{Net-3}}$ are decapsulated and then forwarded to their final destination (SN-D) via the infrastructure mode.

B. Ad Hoc Network Routing Protocol

There is no stationary infrastructure in this network, and even the base stations (MNs) can move randomly around the coverage area. Currently, there are a number of ad hoc routing protocols that have been proposed by the Internet Engineering Task Force (IETF) [8]. These include two prominent on-demand ad hoc routing protocols known as Ad hoc On-demand Distance Vector (AODV) Routing [9] and Dynamic Source Routing (DSR) [10] protocols.

Although both routing protocols share the same on-demand behavior, they are different in terms of routing mechanism. For instance, the DSR uses source routing in hop-by-hop operations, whereas the AODV is based on table-driven routing and destination sequence numbering. The on-demand nature of these protocols simply means that routing discovery begins whenever there is a need to transmit data packets to a destination.

Both protocols have received considerable attention in recent years, and there are a number of publications that have evaluated them in terms of delay, number of nodes, packet transmission rate, and mobility [11], [12]. However, since our main objective in this paper has been to verify the feasibility of the proposed network, we have arbitrarily chosen the AODV routing protocol.

The function of the AODV routing protocol is to discover a routing path between the source and destination MNs. This is performed by means of a route request (RREQ) and route reply (RREP) query cycle. The operation of AODV is described by a simple example depicted in Fig. 5, where the AODV is running within the WLAN network interface associated with each MN. For instance, when a source MN (MN$_{\text{Net-S}}$) requests a route to a destination MN (MN$_{\text{Net-D}}$), it first broadcasts a RREQ packet throughout the ad hoc network. Each node receiving this packet may unicast a RREP to the source if it is either a destination node or an intermediate node (i.e., a hopping node that has a route to another hopping node or the destination node). Otherwise, it rebroadcasts the RREQ and this process continues until the destination node is cached (e.g., MN$_{\text{Net-D}}$). Please note that the nodes that have already received the RREQ, with the same originator IP address and RREQ ID, will ignore the RREQ. In addition, all the receiving nodes refresh their routing table entries with information such as the destination IP address, hop count, precursor, next hop, destination sequence number, etc. [9]. In a continuation of this process, if the source node receives a RREP with a greater sequence number, or the same sequence number with a smaller number of hop counts, it may then update its routing information for that destination. Please note that for a bidirectional link (symmetrical), the same procedure should be repeated in the reverse direction (i.e., MN$_{\text{Net-D}}$-to-MN$_{\text{Net-S}}$).

Once a link between MN$_{\text{Net-S}}$-to- MN$_{\text{Net-D}}$ is established, the route remains active as long as data packets are transmitted from the source MN to the destination MN through the same hopping nodes (MN$_{\text{Net-A}}$, MN$_{\text{Net-B}}$, and MN$_{\text{Net-C}}$). When packets are not transmitted after a certain period of time, the link is no longer considered active and the routing information will be deleted. If a link breakage occurs, which is normally expected due to the mobility nature of the nodes, an error message (RERR) will be sent back to the source. The source then reinitiates the route discovery process.

As soon as the connection is established between the source and destination MNs, the encapsulated IP packets received by the destination MN will then be decapsulated and forwarded to their final destination (i.e., SN).

III. Mobility and Handoff

So far in this network, it has been assumed that all the nodes in a cluster move together (as a group) and SNs will always have the same point of attachment. However, in the case when a mobile node (SN) moves to another cluster, the handoff procedure will occur at the link layer but the change of address support would be needed in order to redirect the IP packet to its new point of attachment. Unfortunately, the current Internet suite of Protocols have been designed on the assumption that the end systems are stationary and change of address makes transparent mobility impossible. This is because Internet routing uses an IP address to identify the point of attachment of the end system device. To achieve transparency, a number of IP-based mobile networking protocols have been proposed [13]. Moreover, the IETF has adopted a mobility system whereby each mobile node retains its home address regardless of its current point of attachment [14]. This is arranged by establishing mobility agents such as Home Agent (HA) and Foreign Agent (FA). For instance, in this network, each SN has a permanent IP address that is attached to its home network (e.g., cluster) and regardless of its current point of attachment, all its receiving packets are first intercepted by the HA.[1] If the destination SN is located at its home cluster, the packets are then forwarded directly to the SN. Otherwise, a care-of-address associated with the FA of the visiting network is used to route the packet to the mobile SN.

[1] It is possible to route packets without going though the HA, which is known as route optimization [23]. Support for route optimization is a fundamental part of Mobile IPv6.

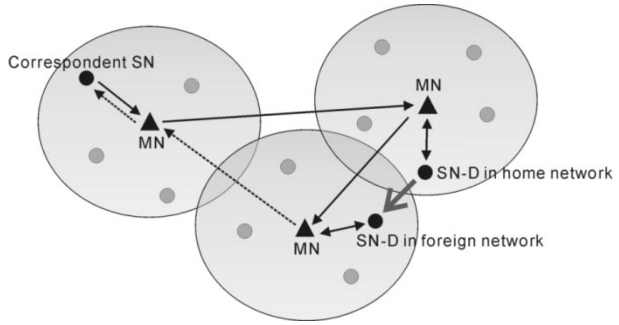


Fig. 6. Handoff via triangle routing for Mobile IPv4.

Forwarding of the packets to the new address is also done via a tunneling process. In this case, the intercepted packets at the home cluster are first encapsulated by adding a new IP header representing the forwarding address as their destination address. The FA in the visiting cluster then deletes the tunnel header and the packets are subsequently delivered to the mobile SN with their original IP address. On the reverse link, the packets can be directly forwarded from the SN to the source node without undergoing the tunneling process. This asymmetrical routing, as shown in Fig. 6, is known as triangle routing. If the source itself is a mobile SN and has moved to a new location with a different point of attachment, the packets transmitted in the reverse direction will go through the same packet redirection process.

As discussed earlier, AODV has the responsibility of establishing the multihop routing to the destination cluster where a mobile SN has been originally registered (see Fig. 6). When the SN moves to a new location covered by a different cluster, the APs are expected to provide seamless roaming. However, for a smooth handoff, the protocol should be able to update the change-of-address registration as quickly as possible to avoid the loss of a large number of packets. The registration process would require updating the care-of-address and the association between the care-of-address of the visiting cluster and the home cluster as well as the registration lifetime. This is known as "*binding*" information, which needs to be updated to support redirecting the packets to the mobile SN. These forwarding procedures, however, can cause handoff latency, whose severity also depends on the MAC layer. Consequently, for real-time applications such video, the handoff latency could cause the loss of a large number of packets, thus affecting the resynchronization of the received video information [20], [21].

However, the mobility can be handled with greater flexibility by utilizing the IP version 6, known as IPv6 [15]. Since a mobile SN can automatically configure its unique IPv6 address in each cluster via stateless address auto-configuration mechanism [19], there is no need to assign an FA in Mobile IPv6. With Mobile IPv6, the source node can receive the binding updates about the change of address and can then send the packets directly to the destination node's new care-of-address using an IPv6 routing header rather than IP encapsulation [16], [17]. In addition, the binding updates can be sent to the MNs in previously visited clusters (including the home cluster) in order to establish forwarding of packets from previous care-of-addresses to the new care-of-address.

At each node, as soon as the interface is up, the auto-configuration process creates a link-local address based on the link-layer address (i.e., MAC address), which normally begin with $\mathrm{fe}80$: prefix. Link-local addresses are special addresses that are only valid on a link of the interface. In other words, the packet with the destination of a link-local address would never pass through a router. Nodes use the Neighbor Discovery protocol [19] to monitor which neighbors are reachable and which are not and to detect their link-layer addresses. With the stateless mechanism each SN then generates its site-local address using locally available information (link-layer address) and information advertised by a IPv6 router (network address). Each SN also sets the link-local address of the router (source address of the router advertisement) as the default gateway (router) in its routing table. When an SN moves to another cluster, it will receive the router advertisement from the MN in this cluster (e.g., via router solicitation). If the prefix does not already exist in the list, the SN creates a new site-local address as described above. Normally, the node uses this new address as the primary address to send packets.[2]

In our implementation, each MN is an IPv6 router and sends router advertisement and router solicitation messages[3] toward its infrastructure network as specified in [19]. This would allow SNs to configure their IPv6 addresses and default gateways (routers) automatically via stateless address autoconfiguration. The gateway of SNs in this case is the IPv6 link-local address of the LAN interface of its corresponding MN. For example, for cluster x, we have used a network prefix $\mathrm{fec}0:0:0:x::/64$. With this network prefix, a node generates an address based on the MAC address. This address is unique as long as each network interface has a unique MAC address. The detailed description of the agent discovery process, registration process, and updating the entries of the routing table is beyond the scope of this paper, but further details can be found in [18], [19].

A. IPv6-in-IPv4 Tunneling

As mentioned earlier, this network is composed of two different types of networks: ad hoc for communication between MNs, and infrastructure for communication between an MN and its associated SNs. For our experimental setup, a combination of IPV4 for AODV[4] and IPv6 for Mobile IP have been considered. In other words, the IPv6 addressing has been used for operation in the infrastructure mode whereas the communication in the ad hoc mode is based on IPv4.

As discussed before, since only MNs are involved in ad hoc routing, a tunneling process would be needed to forward packets from one SN to another via ad hoc routing. In this case, IPv6-in-IPv4 tunneling is used instead of IPv4-in-IPv4 as discussed earlier. As before, the function of IPv6-in-IPv4

[2] Unlike IPv4, IPv6 allows an interface with multiple IP addresses.

[3] The implementation of router advertisement daemon is available at http://v6web.litech.org/radvd.

[4] The use of IPv4 for AODV is mainly due to the unavailability of its IPv6 software implementation for Linux.

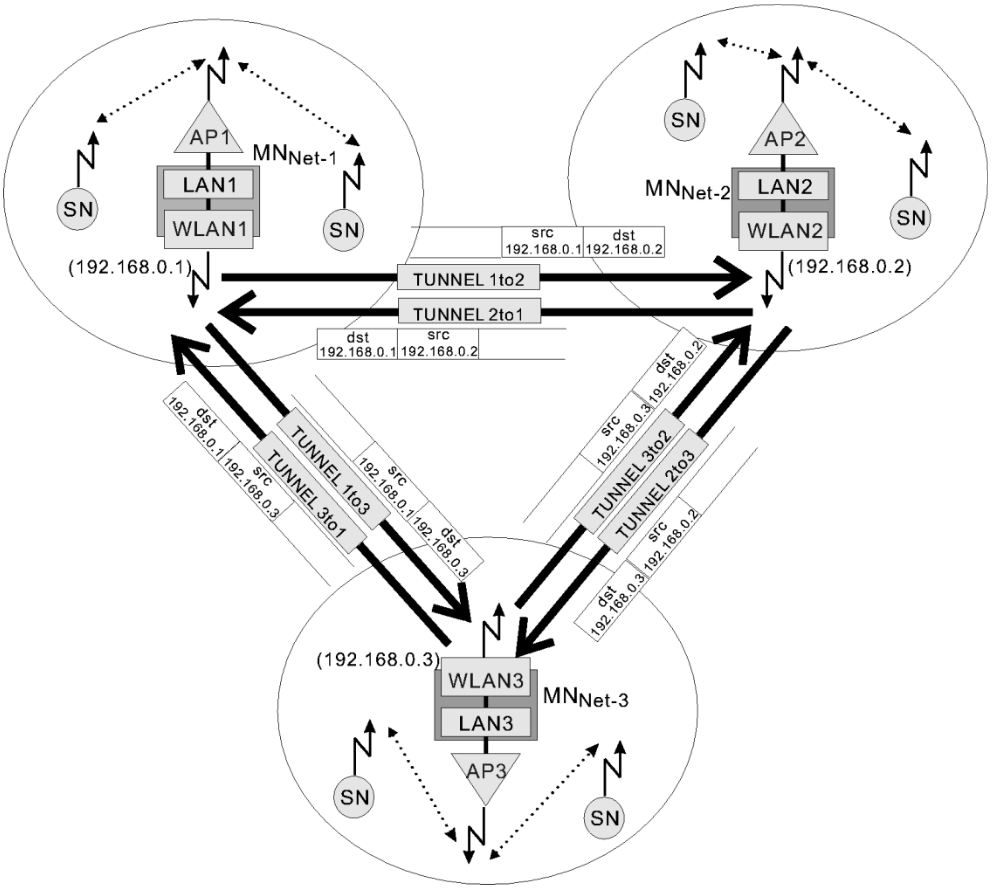


Fig. 7. Example of packet routing using IPv6-in-IPv4 tunneling technique.

tunneling is to encapsulate packets using the source and destination addresses that are allocated for ad hoc routing (i.e., Net-0: $192.168.0.x$, $x = 1, 2, \ldots, 254$).

As an example, let us consider a network where the source SN in cluster x (SN-S$_{\text{Net-}x}$) is sending packets to the destination SN in cluster y (SN-D$_{\text{Net-}y}$). In this case, MN$_{\text{Net-}x}$ encapsulates the IPv6 packets received from SN-S$_{\text{Net-}x}$ and then send them to MN$_{\text{Net-}y}$ $(192.168.0.y)$ by using a new IPv4 header with a source address of $192.168.0.x$. Once these packets arrive at MN$_{\text{Net-}y}$, they are then decapsulated and subsequently forwarded to their destination SN (SN-D$_{\text{Net-}y}$) using their original IPv6 addressing header. For better clarity, Fig. 7 shows the overall IP addressing, including tunneling, for a network of three clusters.

With this arrangement, we were able to apply the Mobile IPv6 protocol to provide a handoff if an SN changes its point of attachment (i.e., moving to a new cluster). As soon as the SN associates with the AP in the new cluster, the SN will then creates a new site-local address (if not created before) by combining a prefix from the router advertisement and the link-layer address. This new address is then used as a primary care-of-address.

B. Network Malfunction

Another form of handoff in this network is arranged to handle a situation when a master node fails to operate properly (e.g., is malfunctioning). This situation would cause the slave nodes that are attached to this master node to lose their communication links with other slave nodes in the network. Let us assume that SN-x is a slave node whose home agent (HA) is MN$_{\text{Net-}x}$ and is currently in its home cluster.

Under these assumptions, as soon as MN$_{\text{Net-}x}$ stops functioning, SN-x will naturally associate itself with the closest master node within its communication range (e.g. MN$_{\text{Net-}y}$ in cluster y). In this case, SN-x can still send packets to other slave nodes that are attached to other clusters. However, a problem arises if other slave nodes attached to different clusters try to send packets to SN-x. This is mainly because other slave nodes cannot update their binding caches for SN-x. Note that under normal handoff conditions, they can send packets to the home address of SN-x, expecting these packets to be forwarded to the right location (if the SN-x is away from home), and the SN-x will eventually send back the binding updates. However, since this process can only be accomplished via the MN$_{\text{Net-}x}$, in its absence, a special arrangement would be needed, as discussed in the following.

This problem can be resolved by assigning multiple home (permanent) addresses to each slave node as a backup. For instance, with IPv6, because each slave node is allowed to have a unique IPv6 address at each cluster, the SN-x could have two home (permanent) addresses belonging to Net-x and Net-z (i.e., Net-x home address and Net-z home address). Equivalently, MN$_{\text{Net-}x}$ and MN$_{\text{Net-}z}$ become the home agents of SN-x. In this case, whenever the SN-x changes its point-of-attachment, it always sends the binding updates (BUs) not only to $\mathrm{MN}_{\mathrm{Net}\text{-}x}$, but also to $\mathrm{MN}_{\mathrm{Net}\text{-}z}$.

With this arrangement, the SN-x will be reachable at least through the $\mathrm{MN}_{\mathrm{Net}\text{-}z}$, even in the absence of $\mathrm{MN}_{\mathrm{Net}\text{-}x}$. For instance, if other slave nodes fail to send packets to the Net-x home address of SN-x, they can simply try an alternative (Net-z) home address. As long as $\mathrm{MN}_{\mathrm{Net}\text{-}z}$ is alive (and there is a route between the SN-x and other slave nodes), they can initially send packets to SN-x through $\mathrm{MN}_{\mathrm{Net}\text{-}z}$ and then directly to SN-x via $\mathrm{MN}_{\mathrm{Net}\text{-}y}$ (after receiving BUs).

IV. IEEE 802.11

The IEEE 801.11 standard defines two different types of radio-frequency-based LANs for the physical layer: direct sequence spread spectrum (DSSS), and frequency hopping spread spectrum (FHSS) [6]. In addition, the standard defines the carrier sense multiple access protocol with collision avoidance (CSMA/CA). The protocol can support WLAN in two different modes: infrastructure and ad hoc. In the infrastructure network mode, mobile nodes should communicate with each other via an AP. Both DSSS and FHSS physical layers can be used to implement this network. The main advantage of using DSSS is to do with its higher throughput rate (up to 11 Mb/s) as compared to 1 or 2 Mb/s FHSS (e.g., using two-level or four-level GFSK modulation) [20]. However, when there is a relatively large number of clusters, the cochannel interference may become a major concern if the DSSS system is deployed. It should be noted that since DSSS can operate in three nonoverlapping channel frequency bands, up to three APs can be collocated without causing too much interference. At the same time, the IEEE 802.11 FHSS system, which hops from narrowband to narrowband (within a wideband), can select one of its 79 possible hopping sequences to avoid interference. Thus, if a larger number of clusters is expected to overlap, the FHSS system may find to be more suitable for the cluster-based network. We should point out that overlapped clusters can occasionally collide on a hop and consequently affect the system throughput. However, the possibility of a large number of clusters moving close to each other to cover a small region depends on the nature of the operation or specific tasks. Nevertheless, when small number of clusters is deployed, the DSSS has the advantage due to lower cost and better throughput rate [6].

Although no attempt has been made in this paper to compare these systems for our application, based on the above observation, we have considered FHSS for the infrastructure part of the network that deploys APs. For the ad hoc part, however, DSSS can also be considered. This is mainly because all the WLAN cards operating in the ad hoc mode (i.e., Net-0) have to use the same hopping sequence in order to communicate with each other. Thus, the DSSS system, with its higher throughput rate, was found to be more suitable for transmission via multihop routing. Nevertheless, such an option has not been considered in our current experimental setup.

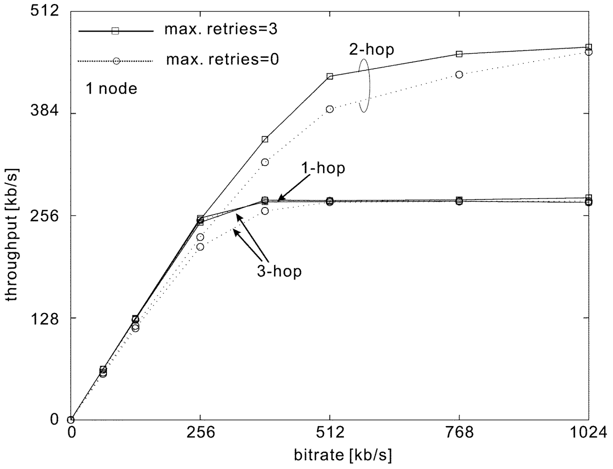


Fig. 8. Throughput performance for one node.

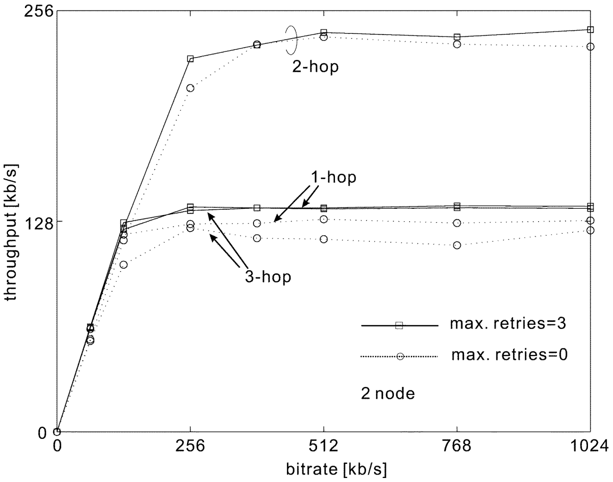


Fig. 9. Throughput performance for two nodes.

Regarding the IEEE 802.11 error correction capabilities, it provides only Automatic Repeat reQuest (ARQ) for the retransmission of corrupted packets. It uses a positive acknowledgment (ACK) when a packet is successfully received without errors. The integrity of a packet is checked by its cyclic redundancy check (CRC) at the receiver. If the transmitting node does not receive an ACK of its packet, it will make more attempts to retransmit the packet. According to the IEEE 802.11 standard [6], the sender is allowed several retransmission attempts.

The retransmission however, may not always be a very effective mechanism for real-time applications, particularly for transmission over multihop networks. Fortunately, the standard has defined a parameter, which could allow the maximum retry attempts to a desirable setting to suit specific applications.

V. Experimental Setup

We have constructed a network consisting of three clusters where each cluster comprises two SN nodes using PDA devices. As mentioned earlier, this network is composed of two networks: ad hoc between MNs and infrastructure between MN and its SNs. The MN is implemented using an IEEE 802.11 FHSS compliant AP, a laptop with an Ethernet

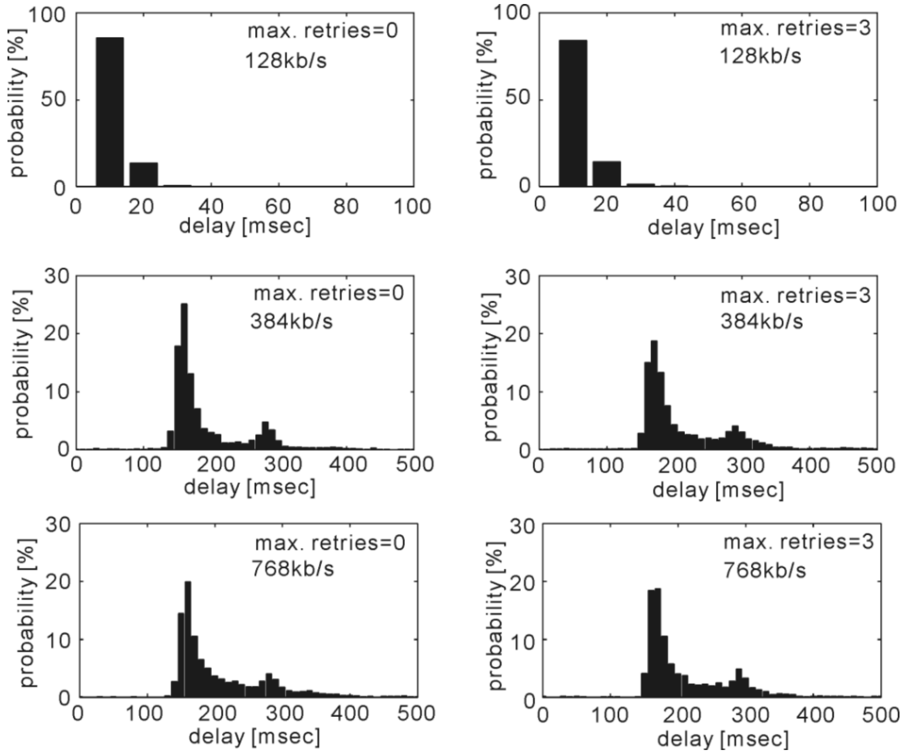


Fig. 10. Propagation delay distributions for 1-hop communication.

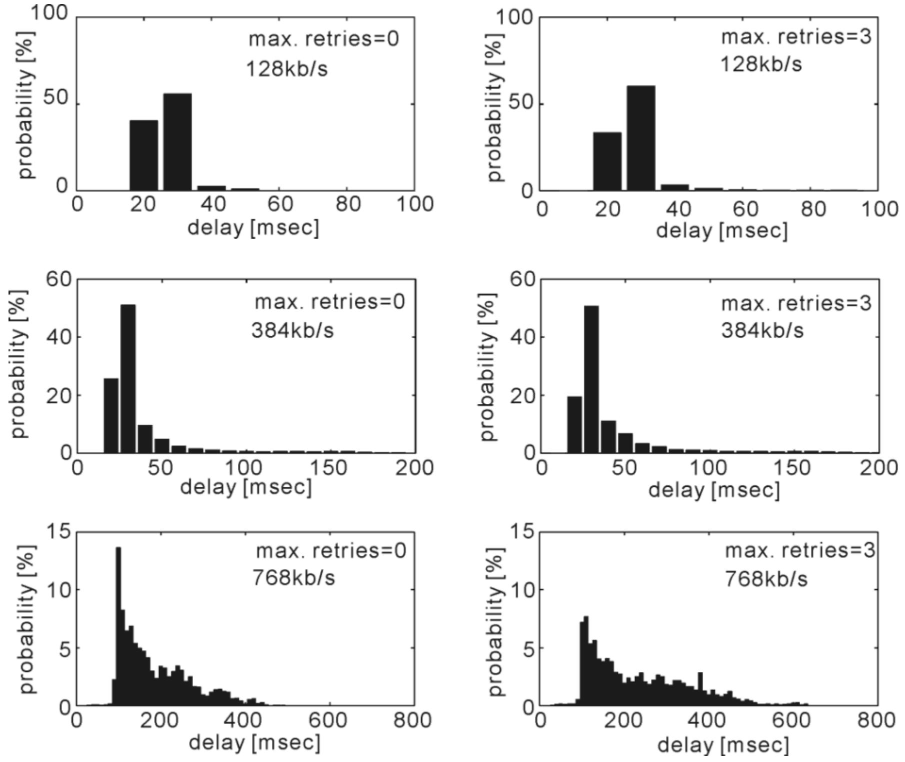


Fig. 11. Propagation delay distributions for 2-hop communication.

port, and an IEEE 802.11 FHSS compliant WLAN card. This Ethernet interface is directly connected to the AP through the cross RJ-45 cable. The SN, which operates in an infrastructure mode, uses an IEEE 802.11 FHSS wireless LAN card and a PDA device. In addition, the data rate for all the IEEE 802.11 FHSS devices have been set to 1 Mb/s. The operating system for the PDAs and laptop PCs is Linux with kernel version 2.4.x, which can function as a router to forward IP packets from the AP (the Ethernet port) to the WLAN card, and vice versa. To evaluate the performance of the proposed network, various tests have been carried out to measure delays and packet-loss rates in a multihop chain transmission.

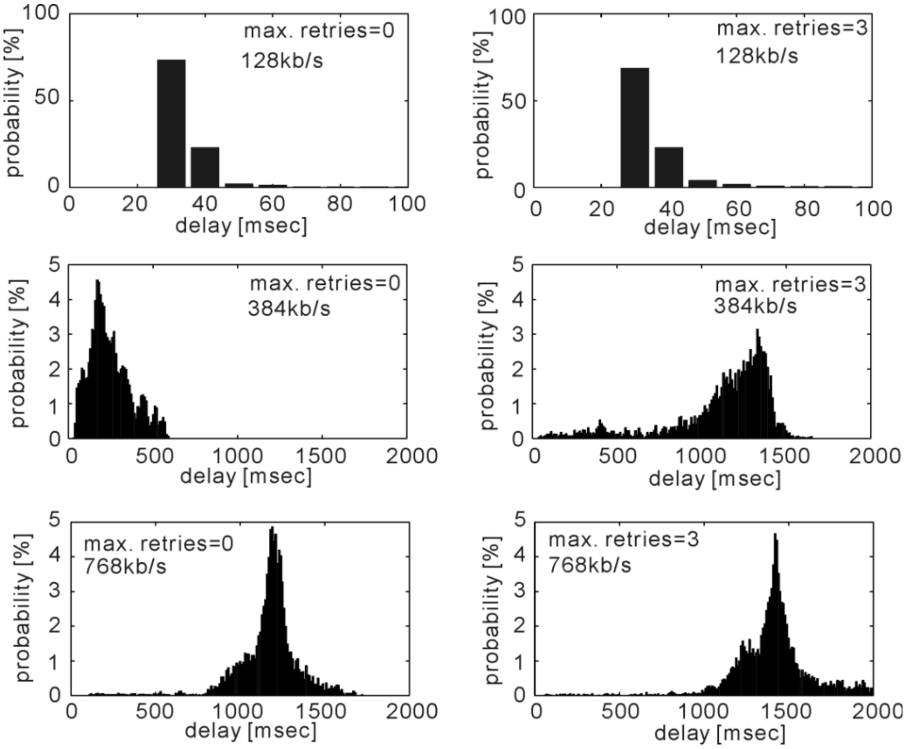


Fig. 12. Propagation delay distributions for 3-hop communication.

In our first set of experiments, the source SN transmits UDP packets to the destination SN. The source SN (SN-S) and the destination SN (SN-D) may belong to the same cluster or attached to different clusters. We define SN-S$_{\text{Net-}j}$ and SN-D$_{\text{Net-}k}$, as the source and destination SNs that are attached to clusters j and k, respectively. The number of MNs that are involved in the transmission defines the number of hops that a packet travels. For instance, if both nodes are located in the same cluster (i.e., $k = j$), the number of hops is one. In this case, communication is performed in an infrastructure mode. It should be noted that the amount of traffic, in this mode, includes transmission from SN-S to the AP and then AP to the SN-D in the same cluster (i.e., 1-hop transmission). As will be shown later, this can affect the throughput performance for the 1-hop as compared with the 2-hop transmission. As more MNs are involved in the transmission process (i.e., via a multihop chain), the cochannel interference may become the main factor affecting the network performance. Such interference could reduce the system throughput as the number of hops increases.

During the first set of experiments, we made sure that for each experiment all the SNs remain within the coverage area of their associated MNs and the nodes remain stationary to prevent any change of routing or handoffs. In addition, since this network has been primarily designed to transmit real-time multimedia information [21], our main objective was to evaluate the effect of the retransmission mechanism that is supported by IEEE 802.11. Thus, in these experiments, the number of maximum retransmissions (*max.retries*) has been set either to 0 (i.e., deactivating the retransmission mechanism), or 3 on all the 802.11 devices. For these measurements, we used the free software "*iperf*"[5] to generate a sequence of 400 bytes length UDP packets at a constant bit rate (CBR).

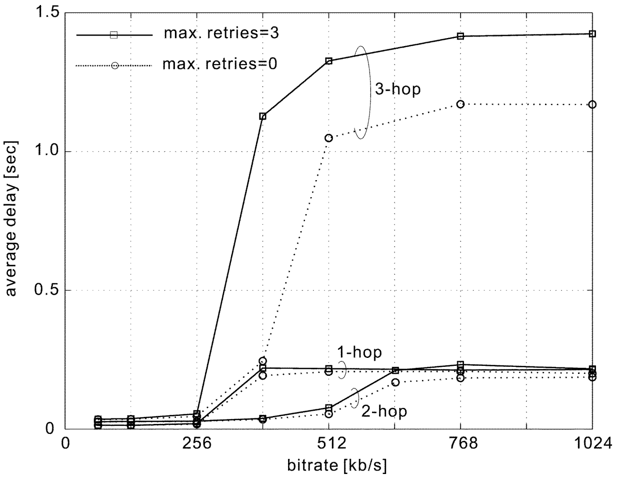
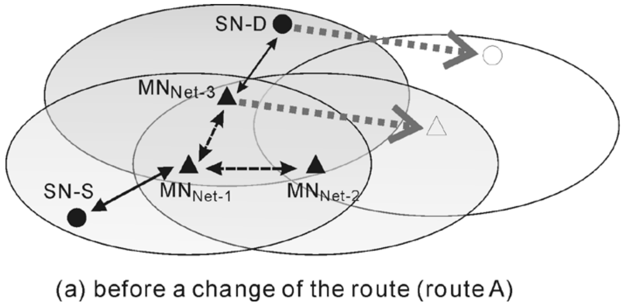


Fig. 13. Average delay.

These tests were carried out many times, and the first set of results are depicted in Figs. 8 and 9. These figures show the system throughput performance when packets are transported via routes with differing number of hops and max.retries when one or two nodes in the same cluster are in contention. Fig. 8 presents the network performance when a single node is involved in the transmission, and Fig. 9 shows the results when two nodes in the same cluster are involved in the simultaneous transmission of real-time data.

[5] This software is available at http://dast.nlanr.net/Project/Iperf



(a) before a change of the route (route A)

(b) after a changing of the route (route B)

Fig. 14. AODV route change scenario.

As can be observed from both figures, at lower bit rates the system throughput increases almost linearly due to lower packet drops. The throughput performance begins to saturate at higher bit rates as the number of transmitting packets can overwhelm the available channel resources. An interesting observation is that the best performance is achieved in the case of 2-hop transmission. As explained earlier, this is due to the higher traffic in a 1-hop transmission as a result of the destination node being in the same cluster.

Regarding retransmission, we noticed that increasing the number of max.retries to 3 cannot significantly improve the network performance. However, at higher bit rates, the retransmission can have a better impact on the throughput performance for the two-nodes case (Fig. 9).

In terms of delay performance, Figs. 10–12 show the measured probability density functions of the end-to-end propagation delays for 1-hop, 2-hop, and 3-hop, respectively. In particular, these figures include the delay distributions for 128, 384, and 768 kb/s with max.retries of 0 and 3. These measurements were based on a time resolution of 10 ms (i.e., 0–10, 10–20, 20–30). We should point out that the propagation delay is the time difference between the received and transmitted packets. We used the Network Time Protocol (NTP)[6] [24] to measure the delays by synchronizing the clock of the source and destination.

The average propagation delays as a function of the source bit rate for 1-hop, 2-hop, and 3-hop with max.retries settings of 1 and 3 are also shown in Fig. 13.

Looking at these figures we can deduce that the average delay remains almost unchanged when the bit rate is much smaller than the system throughput (e.g., $<$256 kb/s). As the bit rate approaches the system throughput, the average delay rises rapidly and then reaches the saturation value. Comparing 1-hop with 2-hop transmission, we notice that the 2-hop has smaller delays at bit rates between 300 and 600 kb/s. This delay increases slightly at higher bit rates (e.g., 768 kb/s). Again, this behavior is due to the fact that 2-hop has smaller peak traffic (i.e., the highest traffic in the channels between the source and destination) than the single hop transmission. In terms of number of max.retries, we noticed that the max.retries of 3 has larger average delays. This is naturally due to the extra delay caused by the retransmission. In particular, the delay further deteriorates with an increase in the number of hops and/or bit rate. Obviously, more hops can cause additional delay and a higher bit rate would result in more backoff time for retransmission due to the increased contention for the channel.

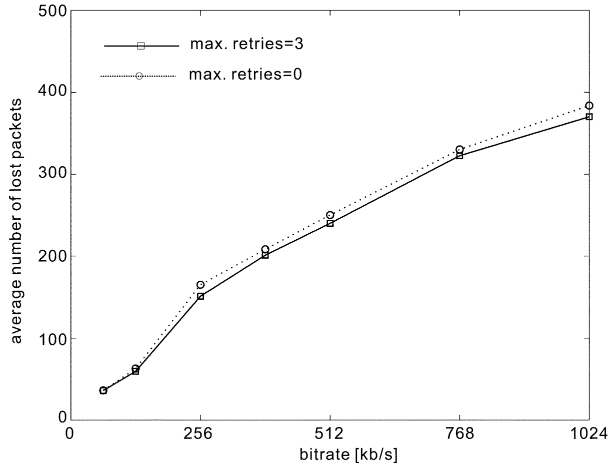


Fig. 15. Average packet loss in AODV route change.

A. Effect of Ad Hoc Routing

Our next set of experiments were mainly concerned with evaluating the effect of ad hoc route change on the network performance. As discussed in Section II-B, the AODV routing protocol has been considered in our experimental setup. For each test, we created an environment where a change of route can occur without causing any handoffs. Fig. 14 presents the test scenario that we used to evaluating the network. Fig. 14(a) shows the initial stage where the source SN (SN-S) in Net-1 sends a sequence of UDP packets to the destination node (SN-D) in Net-3 via MN$_{\text{Net-1}}$ and MN$_{\text{Net-3}}$. As can be observed, there is no intermediate hopping nodes in the ad hoc routing (i.e., direct route between MN$_{\text{Net-1}}$ and MN$_{\text{Net-3}}$), and this has been referred to as route A in Fig. 14(a). Next, we created a situation where a change of ad hoc route can occur during the transmission. In this case, a route change will be via MN$_{\text{Net-2}}$ (intermediate hopping node) referred to as route B in Fig. 14(b).

To make sure that these measurements were performed under the same conditions throughout our experiments, we used a special software tool known as "*mackill*."[7] With this tool, we can intentionally change the routing path by filtering the packets at the MAC layer of the source and the destination nodes (e.g., MN$_{\text{Net-1}}$ and MN$_{\text{Net-3}}$ in this example). In other words, the function of the "*mackill*" is to

[6] The implementation of NTP protocol is available at http://www.ntp.org

[7] This software is available at http://www.apetestbed.sourceforge.net

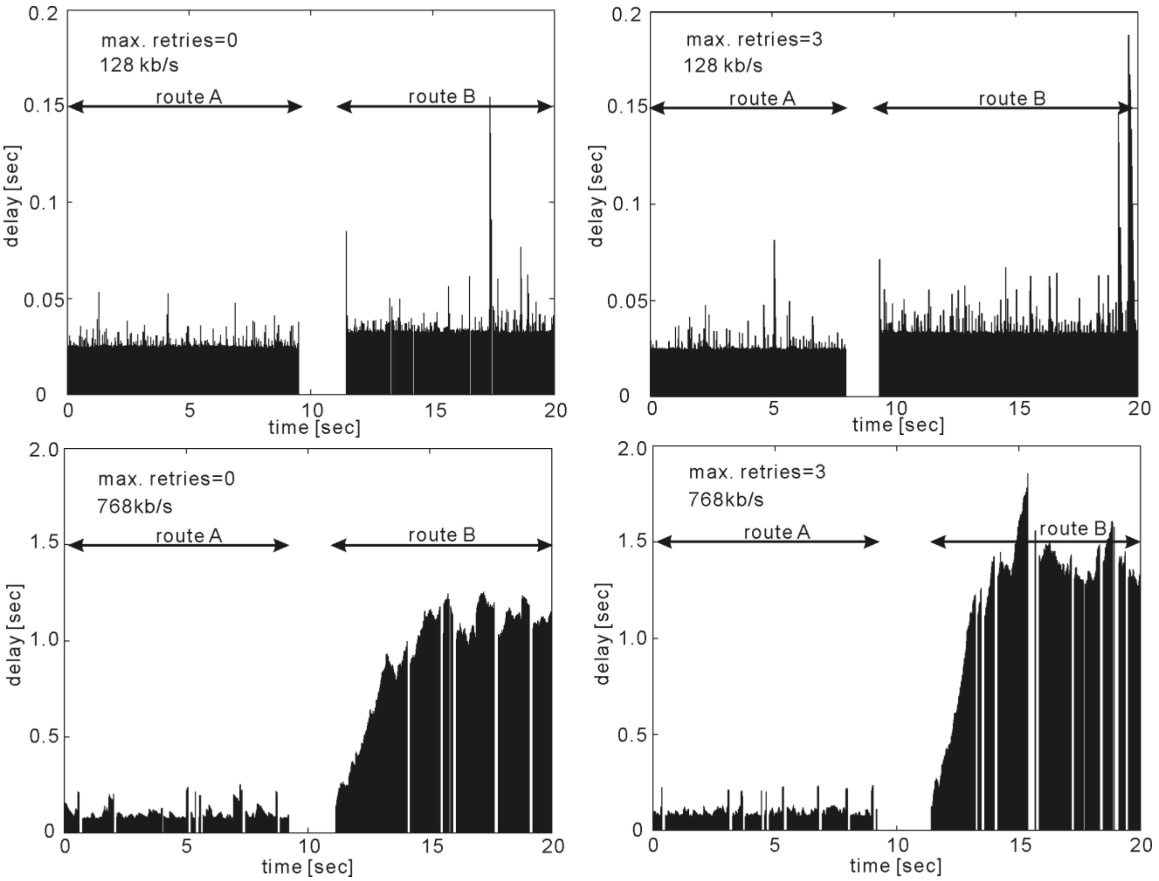


Fig. 16. Delays in AODV route change.

block packets at the MAC layer that are sent from $\mathrm{MN}_{\mathrm{Net}\text{-}1}$ to $\mathrm{MN}_{\mathrm{Net}\text{-}3}$ (and vice versa). This would prevent any communications at the IP layer in which the AODV protocol operates. Consequently, $\mathrm{MN}_{\mathrm{Net}\text{-}3}$ will no longer be considered as $\mathrm{MN}_{\mathrm{Net}\text{-}1}$'s neighbor during the AODV route discovery process. Under such conditions, only $\mathrm{MN}_{\mathrm{Net}\text{-}2}$ will become a neighbor to $\mathrm{MN}_{\mathrm{Net}\text{-}1}$ as $\mathrm{MN}_{\mathrm{Net}\text{-}3}$ to $\mathrm{MN}_{\mathrm{Net}\text{-}2}$ [see Fig. 14(b)]. As soon as the $\mathrm{MN}_{\mathrm{Net}\text{-}1}$ loses its route to $\mathrm{MN}_{\mathrm{Net}\text{-}3}$, $\mathrm{MN}_{\mathrm{Net}\text{-}1}$ sends a RREQ to $\mathrm{MN}_{\mathrm{Net}\text{-}3}$ via its neighboring node, $\mathrm{MN}_{\mathrm{Net}\text{-}2}$. After the route B has been established, the packets sent by SN-S go through route B instead of route A.

It should be noted that the time required to change route from A to B depends on some of the AODV parameters such as ALLOWED_HELLO_LOSS (the number of lost Hello messages that a node can tolerate before considering the link is broken) and HELLO_INTERVAL (the interval between transmitting a hello message) [9]. In these experiments we have used the default values specified in [9] (ALLOWED_HELLO_LOSS $= 2$, HELLO_INTERVAL $= 1000$ ms). Under these conditions, we observed that the time required to change from route A to route B is about 2 s.

It should be noted that despite selecting the above default values for our experiments, these parameters should normally be selected in such a way as to suit specific applications. For instance, ALLOWED_HELLO_LOSS and the HELLO_INTERVAL are parameters that indicate when the link is broken and, thus, more periodic Hello messages can help speeding up the route change or handoff. Consequently, this would be at the expense of higher bandwidth consumption. Therefore, there is a tradeoff when setting the values for these parameters. Nevertheless, we should also point out that it is possible to eliminate the Hello message entirely by relying on the underplaying link layer. For example, in the IEEE 802.11, a node can detect a link failure (to the next hop) by utilizing link layer notifications, such as an absence of ACK, failure to get clear-to-send (CTS) after sending request-to-send (RTS) [6], or overhearing the transmission attempt made by the next hop. Such an arrangement is currently under implementation.

In the first experiment, the average number of missing packets during a route change [e.g., from Fig. 14(a) to (b)] has been measured and the results, as a function of source transmission rate, are shown in Fig. 15. As can be observed, the average packet loss goes up almost linearly as the bit rate increases. This behavior is mainly due to the fact that the time required to change a route is almost the same regardless of the bit rate. Furthermore, comparing the max.retries 0 and 3, we can also observe that the retransmission may not significantly improve the network performance.

In terms of delay performance, Fig. 16 depicts the propagation delays caused by the route change. This figure includes samples for 128 kb/s and 768 kb/s with max.retries 0 and 3. Note that when the bit rate is low (e.g., 128 kb/s), the delays before and after the route change have little effect on

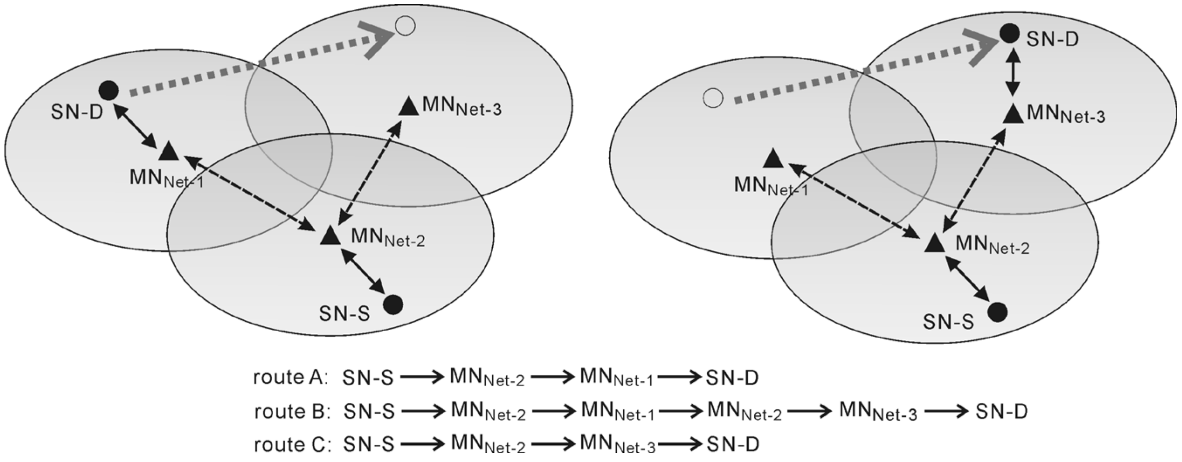

SN-D
MN$_{\text{Net-1}}$
MN$_{\text{Net-2}}$
MN$_{\text{Net-3}}$
SN-S
SN-D
MN$_{\text{Net-1}}$
MN$_{\text{Net-2}}$
MN$_{\text{Net-3}}$
SN-S
route A: SN-S → MN$_{\text{Net-2}}$ → MN$_{\text{Net-1}}$ → SN-D
route B: SN-S → MN$_{\text{Net-2}}$ → MN$_{\text{Net-1}}$ → MN$_{\text{Net-2}}$ → MN$_{\text{Net-3}}$ → SN-D
route C: SN-S → MN$_{\text{Net-2}}$ → MN$_{\text{Net-3}}$ → SN-D

Fig. 17. Handoff with Mobile IP.

the average propagation delays. The average propagation delays at a higher bit rate (i.e., 768 kb/s), as displayed in Fig. 16, increases rapidly before reaching the saturation level around the average delays shown earlier in Fig. 9. This is due to the fact that the traffic in the ad hoc channel immediately after the route change is very low.

B. Handoffs Effect

As discussed in Section III, Mobil IPv6 has been considered for the handoff process. The handoff performance is examined in accordance with the scenario depicted in Fig. 17. In this scenario, MN$_{\text{Net-1}}$ is the home agent of destination SN (SN-D) while the source SN (SN-S) is attached to MN$_{\text{Net-2}}$. Initially, SN-S sends packet to SN-D via MN$_{\text{Net}-2}$ and MN$_{\text{Net-1}}$ (i.e., route A in Fig. 17). Then, SN-D changes its point of attachment by associating with the AP in Net-3 thus triggering a handoff at the link layer. SN-D configures the primary care-of-address (COA) based on the router advertisement from MN$_{\text{Net-3}}$ and its own MAC address. Subsequently, SN-D sends the binding update (BU) to the HA $(\text{MN}_{\text{Net-1}})$ to update its binding cache (BC) for SN-D. Note that to achieve this, MN$_{\text{Net-3}}$ should know the route to MN$_{\text{Net-1}}$. Otherwise, MN$_{\text{Net-3}}$ will send a RREQ to its neighbor, which is MN$_{\text{Net-2}}$ in this case. As soon as the route between MN$_{\text{Net-3}}$ and MN$_{\text{Net-1}}$ (via MN$_{\text{Net-2}}$ which itself hosts the source node in this example) is established, MN$_{\text{Net-1}}$ will send the binding acknowledgment (BA) to MN$_{\text{Net-3}}$. Since at this stage, SN-S does not yet know the change of location of SN-D (assuming SN-D is not yet in the SN-S's BU list), its packets will be intercepted by the HA of the old network $(\text{MN}_{\text{Net-1}})$ before being forwarded to the new COA of SN-D in MN$_{\text{Net-3}}$ (route B). Note that at this stage, the communications between SN-S and SN-D are performed via triangle routing. As soon as SN-D receives the encapsulated packets from MN$_{\text{Net-1}}$, it sends the BU to the sender (SN-S) to notify its new address. SN-S will then update the BC for SN-D in order to send packets directly to SN-D in MN$_{\text{Net-3}}$ (route C).

Under the above test environment, in our first experiment we measured average number of missing packets during the handoff (from MN$_{\text{Net-1}}$ to MN$_{\text{Net-3}}$) as a function of the source UDP bit rate. Fig. 18 shows the average number of missing packets during the handoff. As can be observed, the average number of missing packets increases almost linearly as the bit rate increases. This is because the time required to complete the handoff process almost remains the same, regardless of the source bit rate and max.retries. Note that such behavior may change if there is other traffic in the ad hoc channel.

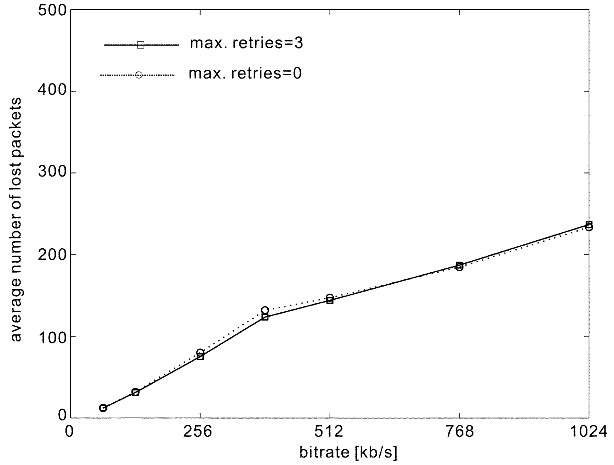


Fig. 18. Average packet loss in Mobile IP.

In our next experiment, we measured the samples of propagation delays versus the transmitted time during the handoff process. These results, which are depicted in Fig. 19, correspond to the time that is required to complete the handoff process. For instance, as SN-D moves to a new cluster, it cannot receive the packets from SN-S until the HA (MN$_{\text{Net-1}}$) updates its BC for the SN-D. This causes packets to be lost for a certain duration. Such a duration depends on the traffic, routes (before and after a handoff), as well as the minimum and maximum router advertisement intervals (MinRtrAdvInterval and MaxRtrAdvInterval) defined in [19]. We used the recommended values of 0.05 and 1.5 for MinRtrAdvInterval and MaxRtrAdvInterval, respectively [19], for the router advertisement at MNs.

After moving to a new cluster, SN-D temporarily receives the packets through the HA (route B). As shown in Fig. 19, the delays are much larger for route B, particularly at the higher bit rates (e.g., 768 kb/s). This is because route B goes

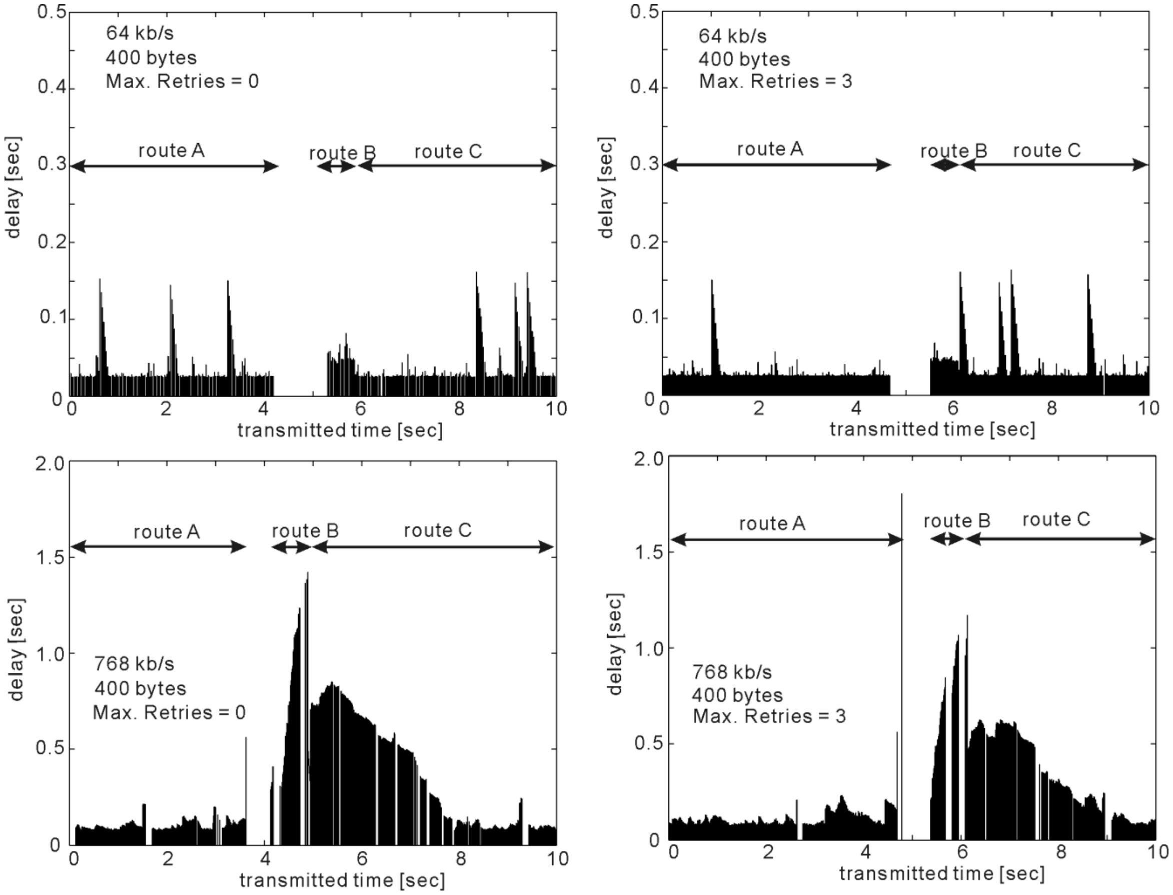


Fig. 19. Delays in Mobile IP.

through more hops than route A and C. Furthermore, within the ad hoc channel, route B is dealing with more traffic than the other routes. For example, compared with route A or C, route B is handling higher traffic in the ad hoc channel because packets go through $\mathrm{MN}_{\mathrm{Net}\text{-}2}$, $\mathrm{MN}_{\mathrm{Net}\text{-}1}$, $\mathrm{MN}_{\mathrm{Net}\text{-}2}$, and $\mathrm{MN}_{\mathrm{Net}\text{-}3}$ (see Fig. 17).

Finally, in our experiments, we observed that the main limiting factor with expanding the number of MNs is the large delay that is mainly caused by a route change in AODV. Consequently, this can result in a loss of many packets, which can have a serious impact for real-time multimedia communication. In addition, as shown in our experiments, packet retransmission, although effective, cannot contribute significantly to recovering the lost packets. For instance, for real-time applications it may become necessary to deploy forward error correction codes at the application layer as well as develop robust error resilient coding for video streaming [20]. Although such an investigation had been carried out during the course of this project, its detailed description is beyond the scope of this paper. However, the experimental setup verifies successful operation of the proposed multihop ad hoc network capable of providing video communication for tactical operations. We hope to measure the network performance when a larger number of clusters have been utilized. In addition, we expect to evaluate the network performance utilizing other ad hoc routing protocols such DSR and optimized link state routing (OLSR) [25].

VI. Conclusion

In this paper, we have proposed a multihop, master-slave cluster-based network architecture. This network has been designed on the assumption that all the nodes within each cluster move as a group. However, to allow handoffs for some isolated nodes, Mobile IPv6 has been considered. The most important feature of the network is that only master nodes are involved in the ad hoc routing. The AODV routing protocol has been used for ad hoc routing.

The paper presents detailed design aspects for the IP-based network for IP version 4 (IPv4) and IP version 6 (IPv6). The network has been implemented using the IEEE 802.11 WLAN technology. An experimental testbed was developed, which was then used to evaluate the performance of the network. This included a number of experiments to measure delays and packet-loss rates under various test scenarios, such as change of routing and handoffs. This network has been primarily developed for video-based sensor networks and has been successfully tested for field trials.

Acknowledgment

The authors wish to thank Prof. L. Hanzo of Southampton University for his constructive comments on this work.

References

[1] A. Ephremides, J. Wieselthier, and D. Baker, "A design concept for reliable mobile radio networks with frequency hopping signaling," *Proc. IEEE*, vol. 75, pp. 56–73, Jan. 1987.

[2] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," *IEEE J. Select. Areas Commun.*, vol. 15, pp. 1265–1275, Sept. 1997.

[3] T. C. Hou and T. J. Tsai, "Distributed clustering for multimedia support in mobile multihop ad hoc networks," *IEICE Trans. Commun.*, vol. E84B, pp. 760–770, Apr. 2001.

[4] J. H. Ryu, S. Song, and D. H. Cho, "Energy-conserving clustering scheme for multicasting in two-tier mobile ad-hoc networks," *Electron. Lett.*, vol. 37, pp. 1253–1255, Sept. 2001.

[5] K. Mase *et al.*, "Flooding schemes for clustered ad hoc networks," *IEICE Trans. Commun.*, vol. E85B, pp. 605–613, Mar. 2002.

[6] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Std 802.11, Aug. 1999.

[7] H. Gharavi and K. Ban, "Master-slave cluster-based multihop ad-hoc networks," *Electron. Lett.*, vol. 37, pp. 1756–1757, Dec. 2002.

[8] Mobile Ad Hoc Network (MANET) Working Group of the Internet Engineering Task Force (IETF).

[9] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad hoc on demand distance vector (AODV) routing," IETF Internet draft, draft-ietf-manet-aodv-13.txt, Feb. 2003.

[10] D. B. Johnson, D. A. Maltz, and Y. C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)," IETF Internet draft, draft-ietf-manet-dsr-08.txt, Feb. 2003.

[11] C. E. Perkins *et al.*, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Pers. Commun.*, vol. 8, pp. 16–28, Feb. 2001.

[12] Y. C. Hu and D. Johnson, "Caching strategies in on-demand routing protocols for wireless ad hoc networks," in *Proc. IEEE/ACM MOBICOM*, Aug. 2000, pp. 231–242.

[13] P. Bhagwat, C. Perkins, and S. Tripathi, "Network layer mobility: an architecture and survey," *IEEE Pers. Commun.*, vol. 3, pp. 54–64, Jun. 1999.

[14] C. Perkins, "IP mobility support for IPv4," IETF Internet draft RFC 3220, Jan. 2002.

[15] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," IETF Internet draft RFC 1883, Dec. 1995.

[16] D. B. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," IETF Internet draft, draft-ietf-mobileip-ipv6-21.txt, Feb. 2003.

[17] R. Koodli, "Fast handovers for MobileIPv6," IETF Internet draft, draft-ietf-mobileip-fast-mipv6-06.txt, Mar. 2003.

[18] S. Thomson and T. Narten, "IPv6 stateless address autoconfiguration," IETF Internet draft RFC2462, Dec. 1998.

[19] T. Narten, E. Nordmark, and W. Simpson, "Neighbor discovery for IP version 6 (IPv6)," IETF Internet draft RFC2461, Dec. 1998.

[20] K. Ban and H. Gharavi, "IEEE 802.11 FHSS receiver design for cluster-based multihop video communications," *Wireless Commun. Mobile Comput.*, vol. 2, pp. 595–605, Sept. 2002.

[21] H. Gharavi and K. Ban, "Video-based multihop ad-hoc sensor network design," in *2002 World Wireless Congr.*, May 2002, pp. 469–474.

[22] A. Kamerman and L. Monteban, "WaveLan-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs Tech. J.*, vol. 2, no. 3, pp. 118–133, 1997.

[23] C. Perkins and D. B. Johnson, "Route optimization in mobile IP," IETF Internet draft, draft-ietf-mobileip-optim-11.txt, Sept. 2001.

[24] D. L. Millis, "Network time protocol (version 3) specification, implementation and analysis," IETF Internet draft RFC1305, Mar. 1992.

[25] C. Adjih *et al.*, "Optimized link state routing protocol," IETF Internet draft, draft-ietf-manet-olsr-08.txt, Mar. 2003.

Hamid Gharavi (Fellow, IEEE) received the Ph.D. degree from Loughborough University, Loughborough, U.K., in 1980.

He joined AT&T Bell Laboratories, Holmdel, NJ, in 1982. He was then transferred to Bell Communications Research (Bellcore) after the AT&T-Bell divestiture, where he became a Consultant on video technology and a Distinguished Member of Research Staff. In 1993, he joined Loughborough University as Professor and Chair of Communication Engineering. Since September 1998, he has been with the National Institute of Standards and Technology (NIST), Gaithersburg, MD. He was a core member of the Study Group XV (Specialist Group on Coding for Visual Telephony) of the International Communications Standardization Body CCITT (ITU-T). He served as a Member of the Communication Sector Panel of the U.K. Technology Foresight Program, Cabinet Office, Office of Science and Technology, from 1994 to 1995. His research interests include video/image transmission, wireless multimedia, mobile communications, ad hoc networks, and third-generation wireless systems. He holds eight U.S. patents related to these topics.

Dr. Gharavi has been an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY since 1996 and has been a Guest Editor for a number of special issues in wireless and multimedia communications. He was an Associate Editor of IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS (1987–1989) and served as Chairman of the VLSI Systems and Applications Committee of the IEEE Circuits and Systems (CAS) Society (1989–1991). Currently, he is a member of the Editorial Board of the PROCEEDINGS OF THE IEEE. He received the Charles Babbage Premium Award of the Institute of Electronics and Radio Engineering in 1986 and the IEEE CAS Society Darlington Best Paper Award in 1989.

Koichiro Ban (Member, IEEE) received the B.S., M.S., and Ph.D. degrees, all in information electronics, from Nagoya University, Nagoya, Japan, in 1996, 1998, and 2001, respectively.

Since April 2001, he has been with the Advanced Network Technology Division, National Institute of Standards and Technology (NIST), Gaithersburg, MD. His research interests include wireless and mobile communications and wireless networking systems.

Dr. Ban is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).